Über Ringe mit Normenadditionsformel

Inaugural-Dissertation

zur

Erlangung des Grades eines Doktors
der Naturwissenschaften

der

Naturwissenschaftlichen Fakultät

der

Julius-Maximilians-Universität
zu Würzburg

vorgelegt von

Artur Bergmann

aus

Braunschweig

R. UNIV.
BIBLIOTHEEK
LEIDEN

Würzburg 1955

Tag der mündl. Prüfung:
5. Juli 1955

Berichterstatter:

Professor Dr. H. L. Schmid

Professor Dr. H. Schmidt

R. UNIV.
BIBLIOTHEEK
LEIDEN

Sonderabdruck aus „Mathematische Nachrichten“
15. Band, Heft 1, Januar 1956
Akademie-Verlag, Berlin

Über Ringe mit Normenadditionsformel*)

Von Artur Bergmann in Braunschweig

(Eingegangen am 12. 8. 1955)

Einleitung

In der arithmetischen Theorie der Korrespondenzen (vgl. Deuring [3] und Roquette [6] zwischen Funktionenkörpern K/Ω und K'/Ω vom Transzendenzgrad 1 über dem algebraisch abgeschlossenen Konstantenkörper Ω entsprechen den gröberen Divisorenklassen des dort betrachteten Doppelkörpers $K \times K'$ eineindeutig Korrespondenzen der Nullklassen von K/Ω in K'/Ω. Diese werden Multiplikatoren genannt. Sind K/Ω und K'/Ω isomorph, so sind diese Multiplikatoren Endomorphismen der Nullklassengruppe von K/Ω und bilden einen Ring, der als Multiplikatorenring M bezeichnet wird.

Die Struktur dieses Multiplikatorenringes M ist von Hasse [5] und Deuring [3] für $g = 1$ (g: Geschlecht des Funktionenkörpers K/Ω) untersucht worden. In M kann eine multiplikative Normfunktion erklärt werden. Mit ihrer Hilfe wird die Strukturuntersuchung durchgeführt, und man kommt zu folgendem Ergebnis: M ist isomorph zu einer Ordnung in einem imaginär-quadratischen Zahlkörper $\mathfrak{Z}$ oder einer Ordnung in einer gewissen Quaternionenalgebra, falls M nicht der Ring der ganzen rationalen Zahlen ist.

Für höheres Geschlecht liegen noch keine solchen Strukturuntersuchungen vor. Die Einführung einer additiven Spurfunktion von A. Weil [9] in die Theorie der Korrespondenzen ist bisher für solche Strukturuntersuchungen nicht verwendet worden.

Man könnte aber vermuten, daß die Struktur des Multiplikatorenringes M für höheres Geschlecht eine Verallgemeinerung des bekannten für $g = 1$ ist, in dem man die dort bekannte Normenadditionsformel in der symmetrischen Schreibweise [1])

$$N(\mu_1 + \mu_2 + \mu_3) - N(\mu_1 + \mu_2) - N(\mu_1 + \mu_3) - N(\mu_2 + \mu_3) + N(\mu_1) + N(\mu_2) + N(\mu_3) = 0$$

*) Dissertation Universität Würzburg 1955; Referenten: Prof. Dr. Hermann Ludwig Schmid, Prof. Dr. Hermann Schmidt.

[1]) Für diese symmetrische Form vergleiche man auch H. L. Schmid [7]. Die Verallgemeinerung für höheres Geschlecht geht auf eine Anregung von Herrn H. L. Schmid zurück.

(μ_1, μ_2, μ_3 seien beliebige Multiplikatoren) in geeigneter Weise verallgemeinert zu

$$\sum_{\nu=1}^{2g+1} (-1)^{2g+1-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(2g+1)} N(\mu_{i_1} + \cdots + \mu_{i_\nu}) = 0.$$

Dabei wird in der inneren Summe über alle Kombinationen $\varkappa \in \mathfrak{K}_\nu(2g+1)$ der $2g+1$ Indizes $1, \ldots, 2g+1$ zur ν-ten Klasse summiert.

$\mu_1, \ldots, \mu_{2g+1}$ sind wieder beliebige Multiplikatoren.

Eine Norm ist für höheres Geschlecht von HASSE bereits eingeführt und von ROQUETTE [6] bei der Untersuchung einer speziellen Frage in M verwendet worden. Dazu muß der zu K/Ω gehörige Abelsche Funktionenkörper herangezogen werden. Ob für diese Norm die vermutete obige Normenadditionsformel erfüllt ist, weiß man nicht.

So wie BEHRBOHM [2] abstrakt die Struktur des Ringes M, der zu $g = 1$ als Multiplikatorenring gehört, untersucht hat, indem er die bekannten Eigenschaften der Norm als Axiome verwendete, soll hier, in Verallgemeinerung dieser Betrachtungen, ein Ring M mit 1-Element, in dem eine Norm mit bestimmten Eigenschaften erklärt ist, auf seine Struktur hin untersucht werden. Könnte man für die im Multiplikatorenring eines Funktionenkörpers eingeführte Norm (oder einer ähnlichen Normfunktion) die hier verwendete Normenadditionsformel beweisen, so wäre die Struktur des Multiplikatorenringes M nach der vorliegenden Arbeit bekannt.

Es soll deshalb in dieser Arbeit ein *Ring* M *mit* 1*-Element* betrachtet werden, in dem *jedem Element* $x \in \mathsf{M}$ *eine ganze rationale Zahl* $[x]$ (die Bezeichnung lehnt sich an WITT [10] an) als *Norm* von x zugeordnet ist. Die *Normfunktion soll drei Axiomen* genügen:

(A_1) $\quad [x \cdot y] = [x][y],$

(A_2) $\quad [x] \neq 0 \quad$ für $\quad x \neq 0,$

(A_3) $\quad \sum_{\nu=1}^{n+1} (-1)^{n+1-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n+1)} [x_{i_1} + \cdots + x_{i_\nu}] = 0 \quad$ „*Normenadditionsformel*“

für beliebige Elemente $x_1, \ldots, x_{n+1} \in \mathsf{M}$ und für eine feste natürliche Zahl n (allgemeiner als oben, wo $n = 2g$ war).

Mit Hilfe dieser Normfunktion werden in Abschnitt I Klammersymbole $(x_1, \ldots, x_k)$ (in Verallgemeinerung derjenigen bei BEHRBOHM [2]) eingeführt und dafür Rechenregeln abgeleitet.

Diese gestatten es dann, für jedes Element $x \in \mathsf{M}$ eine algebraische Gleichung n-ten Grades herzuleiten. Damit ist die Algebraizität von M unter der Voraussetzung der 3 Axiome (A_1), (A_2) und (A_3) nachgewiesen (Satz 1 im Abschnitt II).

Da M die Charakteristik 0 besitzt (I.2), kann in Abschnitt III gezeigt werden, daß sich M *als Ordnung* entweder *in einen Zahlkörper* $\mathfrak{Z}/\mathsf{P}$ vom Grad $m \leqq n$ oder *in eine Divisionsalgebra* $\mathfrak{D}/\mathsf{P}$ von *endlichem Grad* $m_2 \leqq n$ über einen Zahlkörper $\mathfrak{K} \supseteq \mathsf{P}$ einbetten läßt (Satz 2).

Setzt man dann die Normfunktion auf $\mathfrak{Z}$ bzw. $\mathfrak{D}$ fort, so läßt sich die Eindeutigkeit dieser Funktion in $\mathfrak{Z}$ bzw. $\mathfrak{D}$ beweisen (IV. 2). Andererseits kann

man zeigen (IV. 1), daß die *Normenadditionsformel* (A_3) *für die bekannte Norm eines Körpers* $\mathfrak{Z}/\mathfrak{R}$ (wenn $[\mathfrak{Z}:\mathfrak{R}] = n$ ist) bzw. *für die Hauptnorm einer einfachen Algebra* $\mathfrak{A}/\mathfrak{L}$ vom Grad n_2 über dem separablen Zentrum $\mathfrak{K}/\mathfrak{L}$ ($[\mathfrak{K}:\mathfrak{L}] = n_1$; $n_1 \cdot n_2 = n$) *gültig* ist (Satz 3). Dies geschieht mit Hilfe einer Determinantenformel, die den gleichen Aufbau hat wie die Normenadditionsformel.

Damit kann nachgewiesen werden, daß die Normfunktion $[x]$ eindeutig eine Potenz der Körpernorm von $\mathfrak{Z}/\mathsf{P}$ bzw. der Hauptnorm von $\mathfrak{D}/\mathsf{P}$ ist. Auf diese Weise ist einmal gezeigt, daß tatsächlich Ringe M mit den Axiomen (A_1), (A_2) und (A_3) für $n \geqq 2$ existieren und zum anderen nachgewiesen, daß diese Ringe bis auf Isomorphie nur solche Ordnungen in Körpern $\mathfrak{Z}$ bzw. Divisionsalgebren $\mathfrak{D}$ sein können.

Wegen des vermuteten Zusammenhangs mit dem Multiplikatorenring eines Funktionenkörpers werden in Abschnitt V noch *Zusatzaxiome* gefordert (wie sie bei $g = 1$ bekannt sind). Damit erhält man einschränkende Bedingungen für die Zahlkörper $\mathfrak{Z}$ bzw. Divisionsalgebren $\mathfrak{D}$, in die M (wenn auch die Zusatzaxiome erfüllt sind) eingebettet werden kann. Es wird erstens verlangt, daß (A_4) $[x] \geqq 0$ ist (wodurch man n auf $n = 2g$ einschränkt) und außerdem zweitens, daß (A_5) ein involutorischer Antiautomorphismus existiert. Die Existenz eines solchen braucht man für $g = 1$ nicht zu fordern, da in Divisionsalgebren vom Grad 2 immer ein solcher vorhanden ist, was bei höherem Grad nicht der Fall zu sein braucht.

So erhält man das Ergebnis, daß M eine Ordnung in einem Zahlkörper (endlichen Grades) von jeweils bestimmtem Typ bzw. Ordnung in einer gewissen zyklischen Divisionsalgebra mit bestimmten Eigenschaften ist. Diese Typen sind in Abschnitt V am Schluß angegeben. Die bekannten Ergebnisse für $g = 1$ ($n = 2$) sind als Spezialfälle enthalten.

I. Definitionen, Axiome, Rechenregeln für die Klammersymbole

1. *Definitionen und Axiome.*

Es sei M ein Ring mit 1-Element, in dem jedem Element $x \in \mathsf{M}$ eindeutig eine ganze rationale Zahl $[x]$, genannt Norm von x, zugeordnet ist.

Mit Hilfe der Norm $[x]$ werden runde Klammersymbole $(x_1, x_2, \ldots, x_k)$ für eine beliebige natürliche Zahl $k \geqq 2$ folgendermaßen definiert:

$$(D_1) \qquad 2(x, y) = [x + y] - [x] - [y]$$

und für $k \geqq 2$ rekursiv:

$$(D_2) \qquad (k+1)!\,(x_1, \ldots, x_k, x_{k+1}) = k!\,(x_1, \ldots, x_{k-1}, x_k + x_{k+1}) - k!\,(x_1, \ldots, x_{k-1}, x_k) - k!\,(x_1, \ldots, x_{k-1}, x_{k+1}).$$

Für die Norm $[x]$ *seien folgende Axiome erfüllt:*

(A_1) $\quad [x \cdot y] = [x]\,[y]$.

(A_2) $\quad [x] \neq 0 \quad$ für $\quad x \neq 0$.

(A_3) *Es existiert eine feste natürliche Zahl* n, *so daß* $(x_1, x_2, \ldots, x_{n+1}) = 0$ *ist.* „*Normenadditionsformel*“ (x_ν sei beliebig aus M). Dagegen sei $(x_1, \ldots, x_k) \not\equiv 0$ für $k < n + 1$.

Verwendet man (D_1), so folgt aus (D_2) allgemein für die runden Klammersymbole der Ausdruck:

$$(D^*) \qquad k!(x_1, \ldots, x_k) = \sum_{\nu=1}^{k} (-1)^{k-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(k)} [x_{i_1} + \cdots + x_{i_\nu}].$$

Dabei bedeutet Summe über $\varkappa \in \mathfrak{K}_\nu(k)$: Es ist über alle Kombinationen $\varkappa: (i_1, \ldots, i_\nu)$ der k Indizes $1, \ldots, k$ zur ν-ten Klasse zu summieren.

Der Beweis von (D^*) kann durch Induktion nach k erbracht werden. Für $k = 2$ ist (D^*) nach (D_1) richtig. (D^*) sei schon richtig für alle $l \leqq k$.

Nach (D_2) ist dann:

$$(k+1)!(x_1, \ldots, x_{k+1}) = \sum_{\nu=1}^{k} (-1)^{k-\nu} \times$$

$$\times \Big\{ \sum_{\varkappa \in \mathfrak{K}_\nu^1(k)} [x_{i_1} + \cdots + x_{i_\nu}] - \sum_{\varkappa \in \mathfrak{K}_\nu^2(k)} [y_{i_1} + \cdots + y_{i_\nu}] - \sum_{\varkappa \in \mathfrak{K}_\nu^3(k)} [z_{i_1} + \cdots + z_{i_\nu}] \Big\}.$$

Dabei sind die Elemente für:

$$\mathfrak{K}_\nu^1(k) : x_1, \ldots, x_{k-1}, x_k + x_{k+1}$$
$$\mathfrak{K}_\nu^2(k) : x_1, \ldots, x_{k-1}, x_k$$
$$\mathfrak{K}_\nu^3(k) : x_1, \ldots, x_{k-1}, x_{k+1}.$$

Jetzt bildet man in $\mathfrak{K}_\nu^1(k)$, $\mathfrak{K}_\nu^2(k)$, $\mathfrak{K}_\nu^3(k)$ für $1 < \nu < k$ die Kombinationen so, daß zuerst alle diejenigen genommen werden, in denen nur die Elemente $x_1, \ldots, x_{k-1}$ vorkommen.

Für ein festes ν bleibt dann von den drei inneren Summen nur noch $-\sum_{\varkappa \in \mathfrak{K}_\nu(k-1)} [x_{i_1} + \cdots + x_{i_\nu}]$ übrig. Diese Summe erhält also insgesamt das Vorzeichen $(-1)^{k+1-\nu}$.

Dazu nehme man alle Kombinationen zur $(\nu-1)$-ten Klasse aus $\mathfrak{K}_{\nu-1}^1(k)$ mit dem festem Element $x_k + x_{k+1}$ (deren Gesamtvorzeichen jeweils auch $(-1)^{k-1-\nu} = (-1)^{k+1-\nu}$ ist) und alle Kombinationen zur ν-ten Klasse aus $\mathfrak{K}_\nu^2(k)$ und $\mathfrak{K}_\nu^3(k)$ mit festem x_k bzw. x_{k+1} (Gesamtvorzeichen: $(-1)^{k+1-\nu}$). Damit erhält man alle Kombinationen der $k+1$ Elemente $x_1, \ldots, x_k, x_{k+1}$ zur ν-ten Klasse, weil diese so gebildet werden können, daß erst alle Kombinationen der Elemente $x_1, \ldots, x_{k-1}$ genommen werden. Dazu kommen diejenigen, die entweder x_k und x_{k+1} oder x_k bzw. x_{k+1} fest enthalten.

Für $1 < \nu < k$ lassen sich die inneren Summen des obigen Ausdrucks demnach zu

$$(-1)^{k+1-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(k+1)} [x_{i_1} + \cdots + x_{i_\nu}]$$

zusammenfassen.

Für $\nu = 1$ bleiben dann in $\mathfrak{K}_1^1(k)$, $\mathfrak{K}_1^2(k)$, $\mathfrak{K}_1^3(k)$ zusammengefaßt gerade die Elemente $-[x_1], -[x_2], \ldots, -[x_{k-1}]$ mit dem Gesamtvorzeichen $(-1)^k$ und dazu in $\mathfrak{K}_1^2(k)$ und $\mathfrak{K}_1^3(k)$ die Elemente $(-1)^k [x_k]$ bzw. $(-1)^k [x_{k+1}]$ stehen. $\nu = k$ fällt noch unter die obigen Betrachtungen, wenn nur der zweite Teil genommen wird. Dabei bleibt von $\mathfrak{K}_k^1(k)$ nur das Element $[x_1 + \cdots + x_k + x_{k+1}]$ übrig.

Diese drei Einzelbetrachtungen ergeben:

$$(k+1)!(x_1, \ldots, x_{k+1}) = \sum_{\nu=1}^{k+1} (-1)^{k+1-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(k+1)} [x_{i_1} + \cdots + x_{i_\nu}].$$

Damit ist (D^*) aus (D_1) und (D_2) abgeleitet. Kehrt man diese Betrachtung in geeigneter Weise um, so folgt aus (D^*) auch (D_1) und (D_2). Zur Definition der runden Klammersymbole $(x_1, \ldots, x_k)$ sind demnach (D_1) und (D_2) *äquivalent zu* (D^*).

Aus (D^*) folgt vor allem die Symmetrie des Klammersymbols $(x_1, \ldots, x_k)$ in allen vorkommenden Elementen x_ν.

Zum eben angegebenen Axiomensystem ist zu bemerken, daß dadurch keine Bewertung definiert ist, denn $[x + y] \leqq [x] + [y]$ ist nicht erfüllt, wie sich bald für ganze rationale Elemente x, y aus M ergeben wird. (Vgl. (R_{11}) auf S. 62).

2. *Einfache Folgerungen aus den Definitionen und Axiomen.*

(F_1) Aus (A_1) und (A_2) folgt die *Nullteilerfreiheit von* M.
Aus dieser, in Verbindung mit (R_{11}) ist zu schließen, daß M die *Charakteristik* 0 besitzt.

(F_2) $[x] \not\equiv 1$ für alle x aus M, da sonst (A_3) nicht erfüllt ist.
Denn mit $[x] \equiv 1$ folgte aus (D^*)

$$(n+1)!(x_1, \ldots, x_{n+1}) = \sum_{\nu=1}^{n+1} (-1)^{n+1-\nu} \binom{n+1}{\nu} = (1-1)^{n+1} - (-1)^{n+1} \neq 0$$

entgegen (A_3).

(F_3) $[0] = 0$.
Es ist nämlich: $[0 \cdot x] = [0]\,[x] = [0]$ für alle $x \in \mathsf{M}$ (nach (A_1)). Nach (F_2) ist aber $[x] \not\equiv 1$, also $[0] = 0$.

(F_4) $[1] = 1$.
Denn aus (A_1) folgt: $[1 \cdot x] = [1]\,[x] = [x]$ für alle x, also $[1] = 1$.

3. *Das Rechnen mit den Klammersymbolen* $(x_1, \ldots, x_k)$.
$(x, \ldots, y)_k$ bedeutet dabei das Symbol für k Elemente.

(R_1) $(x_1, \ldots, x_k) = 0$ für $k > n + 1$.
Das ist sofort aus (A_3) und (D_2) zu entnehmen, weil dann alle Glieder der rechten Seite gleich 0 werden, wie man durch Induktion nach k feststellt.

(R_2) $(x_1, \ldots, x_k, 0) = 0$.
1. Nach (F_3) ist nämlich $[0] = 0$, d. h. die Behauptung für $k = 1$ aus (D_1) abzulesen.
2. Die Behauptung sei für $l \leqq k - 1$ schon als richtig nachgewiesen, so folgt nach (D_2):

$$(k+1)\,(x_1, \ldots, x_k, 0) = (x_1, \ldots, x_k) - (x_1, \ldots, x_k) - (x_1, \ldots, x_{k-1}, 0) = 0.$$

Daraus folgt speziell:

(R_2') $(0, \ldots, 0)_k = 0$, was man aus (D^*) zusammen mit (F_3) auch ablesen kann.

(R_3) $(x_1, \ldots, x_k) = (x_{i_1}, \ldots, x_{i_k})$ für beliebige Permutationen der Indizes $1, \ldots, k$.

Das ist nur die formelmäßige Darstellung der Bemerkung im Anschluß an den Beweis der Äquivalenz von (D_1) und (D_2) mit (D^*) auf S. 59.

Allgemein braucht man danach eine Regel für $(x_1, \ldots, x_k)$ nur für eine bestimmte Reihenfolge der $x_\varkappa$ abzuleiten.

(R_4) $[x](x_1, \ldots, x_k) = (xx_1, \ldots, xx_k)$.
Das kann aus (A_1) und (D^*) ohne weiteres entnommen werden.

4. *Das Rechnen mit den Symbolen* $(x_1, \ldots, x_n)$.

(R_5) $(x_1, \ldots, x_{n-1}, x_n + y_n) = (x_1, \ldots, x_{n-1}, x_n) + (x_1, \ldots, x_{n-1}, y_n)$.

Das ist sofort aus (D_2) und (A_3) zu ersehen, weil $(x_1, \ldots, x_{n-1}, x_n, y_n) = 0$ ist.

(R_6) $(x_1, \ldots, -x_n) = -(x_1, \ldots, x_n)$.
Setzt man nämlich in (R_5) $y_n = -x_n$, so ist nach (R_2)

$$0 = (x_1, \ldots, x_{n-1}, 0) = (x_1, \ldots, x_{n-1}, x_n) + (x_1, \ldots, x_{n-1}, -x_n).$$

(R_7) Für ganzrationales r gilt: $(x_1, \ldots, x_{n-1}, r \cdot x_n) = r(x_1, \ldots, x_{n-1}, x_n)$.
Das folgt durch wiederholte Anwendung aus (R_5) und (R_6).

(R_8) Für ganzrationale a, b und beliebige x, y aus M ist:

$$(ax + by, \ldots, ax + by)_n = \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu} (\underbrace{x, \ldots, x}_{\nu}, \underbrace{y, \ldots, y}_{n-\nu}).$$

Diese Formel ist eine Folge von (R_3), (R_5) und (R_7), wenn man beachtet, daß $(\underbrace{x, \ldots, x}_{\nu}, \underbrace{y, \ldots, y}_{n-\nu})$ nach Umordnung der Elemente x und y gerade so oft erscheint, wie es Kombinationen von n Elementen zur ν-ten Klasse gibt. (Das ist die Analogie zum binomischen Lehrsatz, nur daß $x^\nu y^{n-\nu}$ hier durch das entsprechende Klammersymbol ersetzt ist).

(R_9) *Multiplikationssatz*:

$$n!(x_1, \ldots, x_n)(y_1, \ldots, y_n) = \sum_{\pi \in \mathfrak{S}(n)} (x_{i_1} y_1, \ldots, x_{i_n} y_n).$$

Dabei ist über alle Permutationen π aus der symmetrischen Permutationsgruppe $\mathfrak{S}(n)$ von n Elementen zu summieren.

Beweis. Es ist

$$P = n!(x_1, \ldots, x_n)(y_1, \ldots, y_n)$$

$$= \left\{ \sum_{\nu=1}^{n} (-1)^{n-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n)} [x_{i_1^{(\nu)}} + \cdots + x_{i_\nu^{(\nu)}}] \right\} (y_1, \ldots, y_n) \qquad \text{(nach } (D^*)\text{)}$$

$$= \sum_{\nu=1}^{n} (-1)^{n-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n)} (\{x_{i_1^{(\nu)}} + \cdots + x_{i_\nu^{(\nu)}}\} y_1, \ldots, \{x_{i_1^{(\nu)}} + \cdots + x_{i_\nu^{(\nu)}}\} y_n)$$

$$\text{(nach } (R_4)\text{)}.$$

Das runde Klammersymbol wird nach (R_5) in eine Summe über Symbole zerlegt, so daß die y_λ jeweils nur einen Faktor $x_{i_\varkappa^{(\nu)}}$ behalten.

Dann wird

$$P = \sum_{\nu=1}^{n} (-1)^{n-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n)} \sum_{v \in \mathfrak{V}_n^{**}(\nu)} (x_{i_1^{(\nu)}} y_1, \ldots, x_{i_n^{(\nu)}} y_n).$$

Die innerste Summe erstreckt sich bei festem ν und bei einer festen Kombination $\varkappa \in \mathfrak{K}_\nu(n)$ über alle Variationen mit Wiederholungen $\mathfrak{V}_n^{**}(\nu)$ der ν Elemente $i_1^{(\nu)}, \ldots, i_\nu^{(\nu)}$, die in $\varkappa \in \mathfrak{K}_\nu(n)$ vorkommen, zur n-ten Klasse. Alle diese Variationen mit Wiederholungen treten bei dieser Zerlegung genau einmal auf.

Auf diese Weise entstehen Klammersymbole der Gestalt $(x_{i_1} y_1, \ldots, x_{i_n} y_n)$, wobei $\{i_1, \ldots, i_n\}$ irgendeine Permutation mit Wiederholungen der Elemente $1, \ldots, n$ ist. Eine feste Permutation mit Wiederholungen $\{i_1, \ldots, i_n\}$ kann unter den $v \in \mathfrak{V}_n^{**}(\nu)$ für verschiedene $\varkappa \in \mathfrak{K}_\nu(n)$ auftreten. Tritt sie unter den $v \in \mathfrak{V}_n^{**}(\nu)$, die zu einem festen $\varkappa \in \mathfrak{K}_\nu(n)$ gehören, überhaupt auf, so genau einmal.

Daher kann man die obige Summe folgendermaßen umformen:

$$P = \sum_{\pi \in \mathfrak{P}^*(n)} (x_{i_1} y_1, \ldots, x_{i_n} y_n) \cdot \sum_{\nu=1}^{n} (-1)^{n-\nu} H_{\mathfrak{K}_\nu(n)}(i_1, \ldots, i_n).$$

Die äußere Summe läuft über alle Permutationen mit Wiederholungen $\mathfrak{P}^*(n)$ der n Elemente $1, \ldots, n$.

$H_{\mathfrak{K}_\nu}(n)\,(i_1, \ldots, i_n)$ ist die Anzahl der Kombinationen $\varkappa \in \mathfrak{K}_\nu(n)$ unter deren zugehörigen Variationen $\{i_1^{(\nu)}, \ldots, i_n^{(\nu)}\} \in \mathfrak{V}_n^{**}(\nu)$ die Permutation $\{i_1, \ldots, i_n\}$ vorkommt.

Es ist jetzt für eine feste Permutation mit Wiederholungen $\{i_1, \ldots, i_n)$ die Zahl $H_{\mathfrak{K}_\nu}(i_1, \ldots, i_n)$ zu berechnen:

Unter den Ziffern $i_1, \ldots, i_n$ seien genau r verschiedene. Dann ist zu bemerken: 1. $\{i_1, \ldots, i_n\}$ kann nur für $\nu \geqq r$ auftreten. 2. $H_{\mathfrak{K}_\nu(n)}(i_1, \ldots, i_n)$ ist dann die Anzahl der Kombinationen $\varkappa \in \mathfrak{K}_\nu(n)$, bei denen die r verschiedenen Ziffern vorkommen, denn dann tritt $\{i_1, \ldots, i_n)$ unter den $v \in \mathfrak{V}_n^{**}(\nu)$ genau einmal auf.

Das sind also die Kombinationen, bei denen auf $\nu - r$ Plätzen beliebige der restlichen $n - r$ Ziffern stehen können. Solche gibt es genau

$$\binom{n-r}{\nu-r} = \binom{n-r}{n-\nu}.$$

Das heißt: Es ist

$$\sum_{\nu=1}^{n} (-1)^{n-\nu} H_{\mathfrak{K}_\nu(n)}(i_1, \ldots, i_n) = \sum_{\nu=1}^{n} (-1)^{n-\nu} \binom{n-r}{n-\nu}$$

$$= \sum_{\varkappa=0}^{n-r} (-1)^{\varkappa} \binom{n-r}{\varkappa} = \begin{cases} 0 & \text{für } r < n \\ 1 & \text{für } r = n. \end{cases}$$

Von den Permutationen aus $\mathfrak{P}^*(n)$ treten in der Gesamtsumme also nur solche mit n verschiedenen Ziffern auf, d. h. die aus $\mathfrak{S}(n)$. Das ist die Aussage von (R_9).

(R_{10}) $(x, \ldots, x)_n = [x]$.

Beweis. In (R_9) setze man $x_1 = \cdots = x_n = 1$. Dann ist $n!(1, \ldots, 1)_n (y_1, \ldots, y_n) = n!(y_1, \ldots, y_n)$ für beliebige y_ν. Da mindestens ein Symbol $(y_1, \ldots, y_n) \neq 0$ ist (vgl. (A_3)), folgt:

$$(1, \ldots, 1)_n = 1 = [1] \quad \text{nach } (F_4).$$

Andererseits ist nach (R_4) und (A_1):

$$[x][1] = [x](1, \ldots, 1)_n = (x, \ldots, x)_n = [x].$$

(R_{11}) Für ganzrationale a, b gilt

$$(a + b, \ldots, a + b)_n = \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu} (1, \ldots, 1)_n = (a + b)^n.$$

Das folgt sofort aus (R_8) und (R_{10}).

Insbesondere gilt also $[r] = r^n$ *für ganzrationales* r.

Jetzt sieht man die Richtigkeit der Bemerkung (S. 59), daß die Axiome in Abschnitt I. 1 keine Bewertung festlegen, ein. Es ist nämlich für $n > 1$ z. B. $[2 + 3] = [5] = 5^n \not\leqq 2^n + 3^n$.

(R_{12}) Aus $(x_1, \ldots, x_{n-1}, x) = 0$ für beliebige $x_1, \ldots, x_{n-1} \in \mathsf{M}$ und ein festes Element x aus M, folgt $x = 0$.

Denn nach (R_{10}) ist $(x, \ldots, x)_n = [x]$. Ist aber $[x] = 0$, so folgt aus (A_2) $x = 0$.

II. Ableitung einer algebraischen Gleichung für ein beliebiges Element $x \in \mathsf{M}$

Satz 1. *Jedes Element x aus einem Ring mit 1-Element, in dem für eine Normfunktion die Axiome (A_1), (A_2) und (A_3) erfüllt sind, genügt einer algebraischen Gleichung n-ten Grades $X(x) = 0$ mit ganzrationalen*[1]) *Koeffizienten und höchstem Koeffizienten 1. Es ist:*

$$X(\zeta) \equiv \sum_{\nu=0}^{n} (-1)^{n-\nu} \binom{n}{\nu} (\underbrace{x, \ldots, x}_{\nu}, \underbrace{1, \ldots, 1}_{n-\nu}) \zeta^{n-\nu}.$$

Der Beweis des Satzes 1 beruht auf (R_{12}). Es wird mit $X(x) \equiv X$ und beliebigen Elementen $y_2, \ldots, y_n \in \mathsf{M}$ gezeigt, daß $(X, y_2, \ldots, y_n) = 0$ ist. Also muß $X = 0$ sein.

Zum Beweis wird demnach folgender Ausdruck betrachtet:

$$Y = n!(X, y_2, \ldots, y_n)$$

$$= n!\left(\sum_{\nu=0}^{n} (-1)^{n-\nu} \binom{n}{\nu} (\underbrace{x, \ldots, x}_{\nu}, \underbrace{1, \ldots, 1}_{n-\nu}) x^{n-\nu}, y_2, \ldots, y_n\right)$$

$$= \sum_{\nu=0}^{n} (-1)^{n-\nu} \binom{n}{\nu} n!(\underbrace{x, \ldots, x}_{\nu}, \underbrace{1, \ldots, 1}_{n-\nu}) (x^{n-\nu}, y_2, \ldots, y_n) \quad (\text{nach } (R_5)).$$

[1]) Formal treten zwar noch Nenner auf, da allg. $n!(x, \ldots, y)_n$ ganzrational ist; vgl. aber den Schluß dieses Abschnitts.

Wird auf das Produkt der Klammersymbole der Multiplikationssatz (R_9) angewendet, so entsteht:

$$Y = \sum_{\nu=0}^{n} (-1)^{n-\nu} \binom{n}{\nu} \sum_{\pi \in \mathfrak{S}^{(\nu)}(n)} (x_{i_1^{(\nu)}} x^{n-\nu}, x_{i_2^{(\nu)}} y_2, \ldots, x_{i_n^{(\nu)}} y_n).$$

Die Bezeichnung $\mathfrak{S}^{(\nu)}(n)$ soll andeuten, daß sich unter den x_{i_λ} gerade ν gleiche Elemente x und $n - \nu$ gleiche Elemente 1 befinden. Unter den $n!$ Permutationen aus $\mathfrak{S}^{(\nu)}(n)$ befinden sich also $\nu!(n-\nu)!$ gleiche.

Daher ist

$$Y = \sum_{\nu=0}^{n} (-1)^{n-\nu} n! \sum_{\pi' \in {}'\mathfrak{S}^{(\nu)}(n)} (x_{i_1^{(\nu)}} x^{n-\nu}, x_{i_2^{(\nu)}} y_2, \ldots, x_{i_n^{(\nu)}} y_n).$$

In der Summe über $\pi' \in {}'\mathfrak{S}^{(\nu)}(n)$ befinden sich jetzt lauter verschiedene Glieder. Die innere Summe wird nun in zwei Summen aufgespaltet:

1. In die Summe mit solchen Klammern, bei denen $x^{n-\nu}$ einen Faktor x erhält,
2. in die, bei denen $x^{n-\nu}$ mit 1 multipliziert wird.

Dabei kann man $(x_{i_1^{(\nu)}} x^{n-\nu}, \ldots, x_{i_n^{(\nu)}} y_n)$ umschreiben in

$$(x \cdot x^{n-\nu}, x y_{i_2}, \ldots, x y_{i_\nu}, y_{i_{\nu+1}}, \ldots, y_{i_n})$$

bzw.

$$(x^{n-\nu}, x y_{i_2}, \ldots, x y_{i_{\nu+1}}, y_{i_{\nu+2}}, \ldots, y_{i_n}).$$

Somit ist

$$Y = \sum_{\nu=0}^{n} (-1)^{n-\nu} n! \sum_{\substack{\pi'_\nu \text{ mit } (\nu-1) \text{ Faktoren } x \text{ bei den } y_{i_\lambda}}} (x \cdot x^{n-\nu}, x y_{i_2}, \ldots, x y_{i_\nu}, y_{i_{\nu+1}}, \ldots, y_{i_n})$$

$$+ \sum_{\nu=0}^{n} (-1)^{n-\nu} n! \sum_{\substack{\pi''_\nu \text{ mit } \nu \text{ Faktoren } x \text{ bei den } y_{i_\lambda}}} (x^{n-\nu}, x y_{i_2}, \ldots, x y_{i_{\nu+1}}, y_{i_{\nu+2}}, \ldots, y_{i_n}).$$

In den inneren Summen stehen nach der obigen Bemerkung über ${}'\mathfrak{S}^{(\nu)}(n)$ wirklich verschiedene Klammersymbole.

Betrachtet man die innere Summe des 1. Gliedes für $\nu + 1$ (d. h. ν Faktoren x bei den y_{i_λ}), so ist sie dieselbe wie die innere Summe des 2. Gliedes für ν, denn es stehen auch dort jeweils ν Faktoren x bei den y_{i_λ}.

Wegen des entgegengesetzten Vorzeichens heben sich deshalb diese beiden inneren Summen in der Gesamtsumme gegenseitig auf für $1 \leqq \nu < n$. Zu untersuchen sind noch:

1. Das Glied $\nu = 0$. Da hier nach Definition kein Faktor x vorkommt, x^n also mit 1 multipliziert wird, kommt dieses Glied definitionsgemäß in der 2. Summe vor und ist somit schon berücksichtigt.

2. Das Glied $\nu = n$. Dieses kommt in der 2. Summe nicht vor, da in diesem Falle alle Plätze einen Faktor x erhalten. Nach der Definition steht dieses Glied in der 1. Summe und ist damit auch verwertet.

Da somit alle Glieder der Gesamtsumme berücksichtigt sind, ist $Y = 0$. Der Beweis des Satzes ist damit erbracht.

Im nächsten Abschnitt wird die Einbettung von M in einen Zahlkörper $\mathfrak{Z}$ bzw. in eine Divisionsalgebra $\mathfrak{D}$ gezeigt. Ist M kommutativ und bezeichnet

man mit $\mathfrak{o}$ die Hauptordnung von $\mathfrak{Z}$, so läßt sich mit Hilfe der Form der Koeffizienten a_ν in $X(\zeta)$ (die formal höchstens den Nenner $\nu!(n-\nu)!$ haben) zeigen, daß für ein bestimmtes ganzrationales Element h die Relation $h\,\mathsf{M} \subseteq \mathfrak{o}$ gilt. Mit Hilfe einer Ganzheitsbasis für $\mathfrak{Z}$ und der Darstellung von $\mathfrak{Z}$ als $\mathfrak{Z} = \mathsf{M}_\Gamma$ (vgl. III. 2) folgt umgekehrt, daß es ein ganzrationales Element g gibt, so daß auch $g\,\mathfrak{o} \subseteq \mathsf{M}$ gilt. Aus diesen beiden Tatsachen folgt nach N. Jacobson (The theory of rings, New York 1943; Ch. X, Theorem 15), daß M in $\mathfrak{o}$ enthalten ist. In ähnlicher Weise folgt auch, daß M nur ganzalgebraische Größen enthält, wenn M nicht-kommutativ ist. Daraus folgt in Verbindung mit IV. 2, daß die Koeffizienten in $X(\zeta)$ ganzrational sind. Im folgenden wird der zu M isomorphe Ring ganzalgebraischer Größen auch mit M bezeichnet.

III. Einbettung von M in einen Zahlkörper bzw. in eine Divisionsalgebra

1. M *sei kommutativ.*

Über die Reduzibilität oder Irreduzibilität der Polynome $X(\zeta)$ kann keine allgemeine Aussage gemacht werden. Zerlegt man die Polynome n-ten Grades in ihre irreduziblen Faktoren, so sei m der *maximale* auftretende *Grad* aller dieser *irreduziblen Bestandteile.* Daß m ein Teiler von n ist, ergibt sich erst in Abschnitt IV. Da M die Charakteristik 0 hat, sind die irreduziblen Gleichungen alle separabel.

Es sei nun $x \in \mathsf{M}$ ein Element, das einer irreduziblen Gleichung vom *Maximalgrad* m genügt. Wird dieses Element dem rationalen Zahlkörper adjungiert, so entsteht der Körper $\mathsf{P}(x)$ vom Grad m über P.

Diesem Körper $\mathsf{P}(x)$ werde jetzt ein weiteres Element $y \in \mathsf{M}$ adjungiert. Da x und y separable Elemente sind, gibt es ein Element $z = ax + by$ (a, b ganzrational), so daß die Beziehung $\mathsf{P}(x, y) = \mathsf{P}(z) \supseteq \mathsf{P}(x)$ besteht. Dieses Element z ist aber aus M und genügt somit einer irreduziblen Gleichung höchstens vom Grad m über P. Also ist $[\mathsf{P}(z):\mathsf{P}] = m$. Wegen $\mathsf{P}(z) \supseteq P(x)$ folgt daher $\mathsf{P}(z) = \mathsf{P}(x)$.

Da y ein beliebiges Element aus M war, folgt daraus $\mathsf{M} \subseteq \mathsf{P}(x)$.

2. M *sei nicht kommutativ.*

m sei wieder der oben erklärte Maximalgrad der irreduziblen Faktoren der Polynome $X(\zeta)$, Z sei das Zentrum von M, Γ der Ring der ganzen rationalen Zahlen.

Es werde nach bekanntem Vorbild (vgl. van der Waerden [8] S. 46) der Quotientenring $\mathsf{M}^* = \mathsf{M}_\Gamma$ durch Einführung der formalen Brüche $\frac{\alpha}{g}$ ($\alpha \in \mathsf{M}$, $g \neq 0 \in \Gamma$) gebildet. Da Γ im Zentrum von M liegt, kann das analog zur Quotientenringbildung mit kommutativen Ringen durchgeführt werden. Ersetzt man dann in geeigneter Weise den zu M isomorphen Unterring von M^* durch M, so hat man also einen M umfassenden Ring M^* gebildet, in dem (nach der entsprechenden Ersetzung) der rationale Zahlkörper P enthalten ist.

Das Zentrum Z^* von M^* ist dann Z_Γ, denn ist $\alpha^* = \frac{\alpha}{g} \in \mathsf{Z}^*$, so ist es speziell mit den Elementen aus Z vertauschbar, also $\alpha \in \mathsf{Z}$. $\mathsf{Z}^* = \mathfrak{K}$ ist nach dem vorigen Unterabschnitt eine endliche algebraische Erweiterung von P.

M^* ist aber auch ein Schiefkörper. Da nämlich $\alpha \in \mathsf{M}$ einer irreduziblen Gleichung höchstens vom Grad m genügt, gilt dasselbe für $\alpha^* = \frac{\alpha}{g}$ über P. Es ist also für jedes $\alpha^* \in \mathsf{M}^*$ $\mathsf{P}[\alpha^*] = \mathsf{P}(\alpha^*)$ ein kommutativer Unterkörper, in dem für α^* ein inverses Element existiert.

Nun werde ein Element $x_1 \in \mathsf{M}^*$ mit *maximalem Grad* m_2 über Z^* gewählt. $\mathsf{K}_1 = \mathsf{Z}^*(x_1)$ ist eine endliche algebraische Erweiterung von P, und es existieren nur endlich viele Zwischenkörper zwischen K_1 und Z^*.

$x_2', \ldots, x_t'$ seien endlich viele Elemente aus M^* mit deren Hilfe man die endlich vielen Zwischenkörper zwischen K_1 und Z^* (die überhaupt mit Elementen aus M^* erzeugbar sind) erzeugen kann. Zu diesen Elementen wähle man $t-1$ Elemente $x_2, \ldots, x_t$, so daß x_ν nicht mit x_ν' vertauschbar ist $(\nu = 2, \ldots, t)$.

Die Teilalgebra $\mathfrak{D} = \mathsf{Z}^*(x_1, \ldots, x_t)$ in M^* besitzt dann das Zentrum $\mathfrak{R} = \mathsf{Z}^*$. Ein maximaler kommutativer Unterkörper dieser Teilalgebra ist $\mathsf{Z}^*(x_1)$ (wegen der Gradvoraussetzung). Also ist $[\mathfrak{D}:\mathsf{Z}^*] = m_2^2$.

Wählt man nun ein beliebiges Element $y \in \mathsf{M}^*$ und bildet $\mathfrak{D}(y)$, so ist wieder $[\mathfrak{D}(y):\mathsf{Z}^*] = m_2^2$, denn es ist $\mathsf{Z}^*(x_1)$ immer noch maximaler kommutativer Unterkörper. Also ist $\mathfrak{D}(y) = \mathfrak{D}$ und somit $\mathfrak{D} = \mathsf{M}^*$. Mit $[\mathsf{Z}^*:\mathsf{P}] = m_1$ ist $m_1 \cdot m_2 = m$.

Nach dem in 1. und 2. gezeigten kann man folgenden Satz formulieren:

Satz 2. *m sei der Maximalgrad der irreduziblen Bestandteile der Polynome $X(\zeta)$ (vgl. Abschnitt II). Dann ist M entweder eine Ordnung in einem Zahlkörper $\mathfrak{Z}$ vom Grad m über P oder eine Ordnung in einer Divisionsalgebra $\mathfrak{D}$ von endlichem Rang über P. $\mathfrak{D}$ ist vom Grad m_2 über seinem Zentrum $\mathfrak{R}$, das ein Zahlkörper vom Grad m_1 über P ist. $m_1 \cdot m_2 = m$.*

Bemerkungen. Ist M kommutativ, so kann M für $m = 1$ der Ring der ganzen rationalen Zahlen sein. Ist M nicht-kommutativ, so ist $\mathfrak{D}$ als Divisionsalgebra von endlichem Grad über einem Zahlkörper von endlichem Grad eine zyklische Algebra. (Vgl. Albert [1], Th. 32, S. 149.)

IV. Realisierung der Norm bei der angegebenen Einbettung und ihre Eindeutigkeit

1. *Normenadditionsformel für die Norm in Körpern bzw. die Hauptnorm in gewissen einfachen Algebren.*

Nachdem man im vorigen Abschnitt die Einbettung kennengelernt hat, entsteht nun die Frage, wie man in diesen Fällen die Norm $[x]$ realisieren kann. Es wird sich zeigen, daß $[x]$ *als geeignete Potenz der zahlentheoretischen Norm bzw. der Hauptnorm* gewählt werden kann.

Zur genaueren Untersuchung wird jetzt folgender Satz bewiesen:

Satz 3. *In einem algebraischen Körper $\mathfrak{Z}$ vom Grad n über dem Körper $\mathfrak{R}$ genügt die Norm $N_{\mathfrak{Z}/\mathfrak{R}}(x)$ der Normenadditionsformel $(x_1, \ldots, x_{n+1}) = 0$.*

Ist $\mathfrak{A}$ eine einfache Algebra über dem Körper $\mathfrak{L}$ vom Rang $n_1 \cdot n_2^2$, $(n_1 \cdot n_2 = n)$, mit dem Zentrum $\mathfrak{R}$, das separabel über $\mathfrak{L}$ ist $([\mathfrak{R}:\mathfrak{L}] = n_1)$, so gilt für die Hauptnorm $N_{H\mathfrak{A}/\mathfrak{L}}(x)$ bezüglich $\mathfrak{L}$ die Normenadditionsformel $(x_1, \ldots, x_{n+1}) = 0$.[1])

[1]) Durch die Spezialisierung $x_1 = x$; $x_2 = \cdots = x_{n+1} = 1$ folgt daraus die Differenzengleichung $\Delta^n N(x) = n!$ für die Norm.

Zum Beweis dieses Satzes wird erst ein *Hilfssatz über Determinanten* abgeleitet.

Hilfssatz. *$Y^{(1)}, \ldots, Y^{(n+1)}$ seien beliebige n-reihige quadratische Matrizen. Dann gilt folgende Relation:*

$$S = \sum_{\nu=1}^{n+1} (-1)^{n+1-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n+1)} det\Big(\sum_{\lambda=1}^{\nu} Y^{(i_\lambda)}\Big) = 0.$$

$\varkappa \in \mathfrak{K}_\nu(n+1)$ sind dabei die Kombinationen der $n+1$ Nummern der Matrizen $1, \ldots, n+1$ zur ν-ten Klasse.

Der Beweis dieses Hilfssatzes beruht auf dem bekannten *Determinantensatz*: s_ν seien die Spalten einer n-reihigen quadratischen Matrix. Es gilt:

$$(*)\quad det(s_1, \ldots, s_i + s_i', \ldots, s_n) = det(s_1, \ldots, s_i, \ldots, s_n) + det(s_1, \ldots, s_i', \ldots, s_n).$$

Zum Beweis des obigen Hilfssatzes werden zuerst die Determinanten, die bei einem beliebigen, für den Augenblick aber festen, System $\mathfrak{K}_\nu(n+1)$ stehen, betrachtet. Es sind Determinanten der Form

$$det\Big(\sum_{\lambda=1}^{\nu} Y^{(i_\lambda)}\Big) = det(s_1^{i_1^{(\nu)}} + \cdots + s_1^{i_\nu^{(\nu)}}, \ldots, s_n^{i_1^{(\nu)}} + \cdots + s_n^{i_\nu^{(\nu)}})$$

$s_l^{i_\lambda^{(\nu)}}$ ist die l-te Spalte der Matrix $Y^{(i_\lambda)}$; $\{i_1^{(\nu)}, \ldots, i_\nu^{(\nu)}\}$ ist eine Kombination $\varkappa \in \mathfrak{K}_\nu(n+1)$.

Auf die obige Determinante wird der Determinantensatz $(*)$ so oft angewendet, bis in jeder Spalte nur noch eine Spalte aus einer der Matrizen $Y^{(i_\lambda)}$ steht. Dann wird

$$det\Big(\sum_{\lambda=1}^{\nu} Y^{(i_\lambda)}\Big) = \sum_{v \in \mathfrak{V}_n^{**}(\nu)} det(s_1^{i_{\lambda_1}^{(\nu)}}, \ldots, s_n^{i_{\lambda_n}^{(\nu)}}).$$

Rechts wird über alle Variationen $v \in \mathfrak{V}_n^{**}(\nu)$ mit Wiederholungen der ν Elemente $i_1^{(\nu)}, \ldots, i_\nu^{(\nu)}$ aus $\varkappa \in \mathfrak{K}_\nu(n+1)$ zur n-ten Klasse summiert.

Das sei nun für alle Glieder $\varkappa \in \mathfrak{K}_\nu(n+1)$ und für alle Indizes $\nu = 1, \ldots, n+1$ durchgeführt. So wird

$$S = \sum_{\nu=1}^{n+1} (-1)^{n+1-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n+1)} \sum_{v \in \mathfrak{V}_n^{**}(\nu)} det(\ldots, s_j^{i_{\lambda_j}^{(\nu)}}, \ldots).$$

Greift man nun, analog wie beim Beweis von (R_9) eine bestimmte Variation mit Wiederholungen $\{i_1, \ldots, i_n\}$ der $n+1$ Elemente $1, \ldots, n+1$ zur n-ten Klasse heraus (die bei verschiedenen Systemen $\mathfrak{V}_n^{**}(\nu)$ auftreten kann), so soll jetzt untersucht werden, wie oft diese mit richtigem Vorzeichen in S auftritt.

Sind r verschiedene Ziffern in der festen Variation $\{i_1, \ldots, i_n\}$, so gilt: Diese Variation kommt nur in den $\varkappa \in \mathfrak{K}_\nu(n+1)$ vor, für die $\nu \geqq r$ ist und die die r fest vorgegebenen Ziffern enthalten. Erscheint die Variation bei den zu $\varkappa \in \mathfrak{K}_\nu(n+1)$ gehörigen $v \in \mathfrak{V}_n^{**}(\nu)$, so dann genau einmal. Die Zahl der Kombinationen $\varkappa \in \mathfrak{K}_\nu(n+1)$, unter deren $v \in \mathfrak{V}_n^{**}(\nu)$ die vorgegebene Variation $\{i_1, \ldots, i_n\}$ erscheint, ist also für festes ν: $\binom{n+1-r}{\nu-r}$. Die Gesamt-

anzahl A für alle ν ist also (mit jeweils richtigem Vorzeichen):

$$A = \sum_{\nu=r}^{n+1} (-1)^{n+1-\nu} \binom{n+1-r}{\nu-r}.$$

Mit $\lambda = n+1-\nu$ ergibt sich:

$$A = \sum_{\lambda=0}^{n+1-r} (-1)^{\lambda} \binom{n+1-r}{n+1-r-\lambda} = 0 \quad \text{für} \quad r = 1, \ldots, n.$$

Und nur für solche Werte von r interessiert hier diese Summe. Das heißt aber, daß sich die Determinanten $det(s^{i}_{1}, \ldots, s^{i_n}_{n})$ für eine beliebige Variation (mit Wiederholungen) $\{i_1, \ldots, i_n\}$ der $n+1$ Elemente $1, \ldots, n+1$ zur n-ten Klasse in S gegenseitig aufheben. Der Hilfssatz über Determinanten ist damit bewiesen.

Der Beweis des oben angegebenen *Satzes* über die Norm ergibt sich nun so:

1. $\mathfrak{Z}$ *sei ein algebraischer Körper vom Grad* n *über* $\mathfrak{R}$. Denkt man sich dann die reguläre Darstellung von $\mathfrak{Z}$ in $\mathfrak{R}$ gegeben, die vom Grad n ist, so wird die Norm für ein Element x aus $\mathfrak{Z}$ bezüglich $\mathfrak{R}$ die Determinante der Darstellungsmatrix. Nach dem Hilfssatz gilt dann die Normenadditionsformel $(x_1, \ldots, x_{n+1}) = 0$. Denn diese hat dieselbe Form wie die Relation im Hilfssatz.

Aus diesen Betrachtungen kann man allgemeiner folgern, daß für die k-te *Potenz der Norm die Normenadditionsformel* $(x_1, \ldots, x_{k \cdot n+1}) = 0$ gilt. Dazu braucht man nur eine Darstellung von $\mathfrak{Z}$ in $\mathfrak{R}$ vom Grad $k \cdot n$, die die reguläre Darstellung gerade k-mal enthält, heranzuziehen. Die Darstellungsmatrix enthält längs der Hauptdiagonalen die reguläre Darstellung k-mal, so daß die Determinante die k-te Potenz der Determinante der regulären Darstellung ist, woraus die Behauptung folgt.

2. $\mathfrak{A}$ *sei eine einfache Algebra über dem Körper* $\mathfrak{L}$ *mit einem über* $\mathfrak{L}$ *separablen Zentrum* $\mathfrak{K}$.

Ist dann $[\mathfrak{A}:\mathfrak{K}] = n_2^2$, $[\mathfrak{K}:\mathfrak{L}] = n_1$, $n_1 \cdot n_2, = n$, so gilt nach Deuring [4], S. 50/51: Das Minimalpolynom der Algebra $\mathfrak{A}/\mathfrak{L}$ ist irreduzibel vom Grad n. Die Hauptgleichung eines Elementes $a \in \mathfrak{A}$ ist die charakteristische Gleichung einer Matrix A vom Grad n.

Nach diesem Satz ist die Hauptnorm $N_{H\mathfrak{A}/\mathfrak{L}}(a)$ eines Elementes $a \in \mathfrak{A}$ bezüglich $\mathfrak{L}$ die Determinante von A. Dann gilt nach dem Hilfssatz die Normenadditionsformel für die Hauptnorm. Für die Potenz der Hauptnorm gilt das Analoge wie oben für die Körpernorm.

Der *Satz* 3, der damit bewiesen ist, ist nicht nur eine Aussage für die Norm in Körpern bzw. Algebren. Er besagt andererseits auch die *Existenz* einer *Normfunktion*, die die *Axiome* (A_1), (A_2) und (A_3) erfüllt. Das war von vornherein nicht bekannt.

2. *Die Eindeutigkeit der Norm* $[x]$ *und ihre Realisierung.*

a) M *sei kommutativ, d. h. eingebettet in* $\mathfrak{Z}/\mathsf{P}$, wobei $[\mathfrak{Z}:\mathsf{P}] = m$ ist. (Vgl. Abschnitt III. 1.)

$ax + by + \cdots + hz$ $(x, y, \ldots, z \in \mathsf{M};\ a, b, \ldots, h \in \Gamma)$ sei eine endliche Summe. Wendet man die Regeln (R_{10}) $(x, \ldots, x)_n = [x]$

$$(R_5) \qquad (x_1, \ldots, x_n + y_n) = (x_1, \ldots, x_n) + (x_1, \ldots, y_n)$$

und (R_7) $(x_1, \ldots, r \cdot x_n) = r(x_1, \ldots, x_n)$ auf den Ausdruck

$$(ax + by + \cdots + hz, \ldots, ax + by + \cdots + hz)_n = [ax + by + \cdots + hz]$$

an, so erkennt man, daß die Norm $[x]$ eine Form n-ten Grades in den Koeffizienten $a, b, \ldots, h$ ist. Das ist eine Verallgemeinerung von (R_{10}).

Legt man daher eine Basis $\theta_1, \ldots, \theta_m$ für M zugrunde, so ist demnach $[x]$ als *Form* n-ten Grades *in den Komponenten* $x_\nu \in \Gamma$ von $x = \sum_{\nu=1}^{m} x_\nu \theta_\nu$ darstellbar. Diese Form werde mit $F(x) \equiv F(x_1, \ldots, x_m)$ bezeichnet.

$[x]$ ist in M demnach eine Funktion mit folgenden Eigenschaften:

(E_1) Sie ist darstellbar als Form $F(x_1, \ldots, x_m)$ in den Komponenten von x (wenn eine bestimmte Basis gewählt ist).

(E_2) Sie erfüllt die Funktionalgleichung $\varphi(x \cdot y) = \varphi(x)\varphi(y)$ (nach (A_1)).

Mit $\varphi(x)$ werde nun allgemein eine Funktion in M bezeichnet, die die Eigenschaften (E_1) und (E_2) besitzt.

Vermöge der Eigenschaft (E_1) läßt sich $\varphi(x)$ auf $\mathfrak{Z}/\mathsf{P}$ fortsetzen, indem man für die Komponenten $x_\nu \in \Gamma$ in $F(x_1, \ldots, x_m)$ auch beliebige rationale Zahlen zuläßt. Dabei sei $F(x_1, \ldots, x_m)$ die der Funktion $\varphi(x)$ (nach (E_1)) zugeordnete Form bezüglich einer bestimmten Basis.

Die Funktionalgleichung (E_2) bleibt dabei erhalten. Der Einfachheit halber wird nun die auf $\mathfrak{Z}/\mathsf{P}$ fortgesetzte Funktion wieder mit $\varphi(x)$ bezeichnet.

Zum Beweis der *Eindeutigkeit der Normfunktion* $[x]$ wird nun folgender Weg eingeschlagen:

1. Es wird gezeigt, daß eine Funktion $\varphi(x)$ mit den oben bezeichneten Eigenschaften (E_1) und (E_2) notwendig eine Potenz der Norm $N_{\mathfrak{Z}/\mathsf{P}}(x)$ ist. Daß man dabei $\varphi(x)$ als eine Funktion in $\mathfrak{Z}/\mathsf{P}$ betrachten kann, folgt aus der obigen Fortsetzung von $\varphi(x)$ auf $\mathfrak{Z}/\mathsf{P}$.

2. Der Exponent in der Potenz von $N_{\mathfrak{Z}/\mathsf{P}}(x)$ wird festgelegt durch die bekannte Tatsache von (R_{11}), daß $\varphi(r) = r^n$ sein muß, wenn r aus Γ ist.

Dadurch ist eine Funktion $\varphi(x)$ mit den Eigenschaften (E_1) und (E_2) und der weiteren, daß sie mit $[x]$ für alle rationalen Argumente r übereinstimmt, eindeutig als eine bestimmte Potenz der Norm $N_{\mathfrak{Z}/\mathsf{P}}(x)$ festgelegt.

3. Da die Norm $N_{\mathfrak{Z}/\mathsf{P}}(x)$ und ihre Potenzen nach Abschnitt IV. 1 aber auch die Normenadditionsformel erfüllen, andererseits $[x]$ eine solche Funktion $\varphi(x)$ ist, ist damit $[x]$ eindeutig als $[x] = N^{n'}_{\mathfrak{Z}/\mathsf{P}}(x)$ bestimmt.

Es ist also zuerst zu zeigen:

In $\mathfrak{Z}/\mathsf{P}$ sei eine Funktion $\varphi(x)$ mit den Eigenschaften (E_1) und (E_2) definiert. Dann ist $\varphi(x) = N^{n'}_{\mathfrak{Z}/\mathsf{P}}(x)$. (Da $\mathfrak{Z}$ hier fest vorgegeben ist, wird $N_{\mathfrak{Z}/\mathsf{P}}(x)$ kurz mit $N(x)$ bezeichnet).

Zu diesem Zweck wird $\mathfrak{Z}/\mathsf{P}$ als Algebra über P aufgefaßt und eine Grundkörpererweiterung von P auf P^* vorgenommen: $\mathfrak{Z} \times \mathsf{P}^*/\mathsf{P}^*$.

Zufolge der Eigenschaft (E_1) läßt sich $\varphi(x)$ auf $\mathfrak{Z} \times \mathsf{P}^*/\mathsf{P}^*$ fortsetzen. Die Eigenschaft (E_2) bleibt dabei erhalten. Um das zu zeigen, werde die Eigenschaft (E_2) als eine Polynomidentität in folgender Weise ausgedrückt:

Es sei $\theta_1, \ldots, \theta_m$ eine Basis für $\mathfrak{Z}/\mathsf{P}$ und damit eine für $\mathfrak{Z} \times \mathsf{P}^*/\mathsf{P}^*$. Mit Hilfe dieser Basis werden nun Polynome $\chi_\varkappa(\xi, \eta)$ in den Unbestimmten ξ_ν, η_ν $(\nu = 1, \ldots, m)$ definiert durch das Produkt:

$$\left(\sum_{\nu=1}^{m} \xi_\nu \theta_\nu\right)\left(\sum_{\nu=1}^{m} \eta_\nu \theta_\nu\right) = \sum_{\varkappa=1}^{m} \chi_\varkappa(\xi, \eta)\theta_\varkappa$$

(E_2) ist nun (gleichgültig, welcher Grundkörper gewählt wird) gleichbedeutend mit der Polynomidentität

$$(I_1) \qquad F(\ldots, \chi_\varkappa(\xi, \eta), \ldots) = F(\ldots, \xi_\nu, \ldots) F(\ldots, \eta_\nu, \ldots),$$

wobei F wieder die zu $\varphi(x)$ gehörige Form bezüglich der Basis $\theta_1, \ldots, \theta_m$ ist.

Diese Beziehung ist aber für den rationalen Grundkörper P erfüllt, also auch für jeden Erweiterungskörper P^* von P.

Jetzt wählt man als P^* die galoissche Hülle Ω von $\mathfrak{Z}$. Dann zerfällt $\mathfrak{Z} \times \Omega/\Omega$ vollständig in der Gestalt $\sum_{\nu=1}^{m} \Omega\varepsilon_\nu$ mit orthogonalen, idempotenten Elementen ε_ν (vgl. z. B. Albert [1], S. 31).

Schreibt man nun die Funktion $\varphi(x)$ (in $\mathfrak{Z} \times \Omega/\Omega$) als Form $\tilde{F}$ n-ten Grades bezüglich der Basis $\varepsilon_1, \ldots, \varepsilon_m$, so nimmt (I_1) die Form

$$(I_2) \qquad \tilde{F}(\ldots, \xi_\varkappa\eta_\varkappa, \ldots) = F(\ldots, \xi_\varkappa, \ldots) F(\ldots, \eta_\varkappa, \ldots)$$

an, weil für diese Basis $\chi_\varkappa(\xi, \eta) = \xi_\varkappa\eta_\varkappa$ ist.

Aus (I_2) folgt aber notwendig, daß $\tilde{F}$ von der Gestalt $\tilde{F} = c \cdot \prod_{\nu=1}^{m} x_\nu^{n_\nu}$ ist. (Die x_ν sind die Komponenten von x bezüglich der Basis $\varepsilon_1, \ldots, \varepsilon_m$). Besteht nämlich $\tilde{F}$ aus k verschiedenen Monomen, so stehen auf der linken Seite von (I_2) k, auf der rechten Seite aber k^2 Monome. Das ist nur für $k = 1$ möglich. Ebenso folgt $c = 1$, denn wegen der Funktionalgleichung (E_2) muß $c^2 = c$ sein.

Es ist jetzt noch zu zeigen, daß die Exponenten n_ν alle gleich sind. Denn es ist $N(x) = \prod_{\nu=1}^{m} x_\nu$. Sind alle $n_\nu = n'$, so ist die Behauptung über $\varphi(x)$ bewiesen.

Zu diesem Zweck wird die Form $\tilde{F}$ auf eine bestimmte Basis $1, \theta, \ldots, \theta^{m-1}$, wobei θ bereits in $\mathfrak{Z}$ liegt, zurücktransformiert. Dann muß eine Form mit Koeffizienten aus P entstehen. Die Transformation auf die Basis $1, \theta, \ldots, \theta^{m-1}$ geschieht dadurch, daß in $\tilde{F}$ auf die x_ν eine lineare Transformation

$$(x_1, \ldots, x_m) = (y_1, \ldots, y_m) \cdot \mathsf{T}$$

ausgeübt wird.

Die Klammern $(x_1, \ldots, x_m)$ und $(y_1, \ldots, y_m)$ sind als einreihige Matrizen aufzufassen. Die y_ν sind die neuen Komponenten von x bezüglich der Basis $1, \theta, \ldots, \theta^{m-1}$.

Die Matrix T ist dabei durch die Basistransformation

$$\begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{m-1} \end{pmatrix} = \mathsf{T} \begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_m \end{pmatrix}$$

festgelegt.

Es wird dann $\widetilde{F}(x_1, \ldots, x_m) = \prod_{\nu=1}^{m} L_\nu^{n_\nu}(y) \equiv F(y_1, \ldots, y_m)$.

Die $L_\nu(y)$ sind Linearformen mit Koeffizienten aus Ω und entsprechen den Spalten von T. Wendet man nun die Automorphismen von Ω/P auf $F(y_1, \ldots, y_m)$ an, so wird behauptet, daß die L_ν transitiv permutiert werden. $F(y_1, \ldots, y_m)$ bleibt als Polynom mit Koeffizienten aus P dabei aber fest. Also müssen die n_ν notwendig alle gleich sein, da die L_ν den Charakter von Unbestimmten haben.

Es ist nur noch zu zeigen, daß die L_ν (d. h. die Spalten von T oder, was dasselbe ist, die Zeilen von T^{-1}) transitiv permutiert werden.

Dazu geht man von der Beziehung

$$\begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_m \end{pmatrix} = \mathsf{T}^{-1} \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{m-1} \end{pmatrix}$$

aus.

$\Phi(x)$ sei das irreduzible Polynom mit der Nullstelle θ. Man denke sich dann die Algebra $\mathfrak{Z} \times \Omega/\Omega$ als Restklassenring nach dem Ideal $(\Phi(x))$ dargestellt. Bildet man in $\Omega[x]$ die Polynome

$$\psi_i(x) = \frac{\Phi(x)}{x - \xi_i} \frac{1}{\Phi'(\xi_i)} \qquad (i = 1, \ldots, m)$$

wobei die ξ_i die verschiedenen Nullstellen von $\Phi(x) = 0$ sind, so kann $\varepsilon_i = \psi_i(x)$ gesetzt werden (vgl. Albert [1], S. 31).

Die Matrix T^{-1} entsteht also aus der Beziehung

$$\begin{pmatrix} \psi_1(x) \\ \vdots \\ \psi_m(x) \end{pmatrix} = \mathsf{T}^{-1} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{m-1} \end{pmatrix}.$$

Da die $\psi_i(x)$ bei Automorphismen von Ω/P transitiv permutiert werden, so auch die Zeilen von T^{-1}.

Damit ist gezeigt, daß eine Funktion $\varphi(x)$ in $\mathfrak{Z}/\mathsf{P}$ mit den Eigenschaften (E_1) und (E_2) notwendig eine Potenz der Norm $N(x)$ sein muß.

Der oben angegebene Schritt (1) zur Bestimmung der Eindeutigkeit von $[x]$ ist also erledigt.

Für (2) wird (R_{11}) berücksichtigt. Dann muß $\varphi(r) = r^n = N^{n'}(r) = r^{m \cdot n}$ sein. Die Potenz wird demnach durch $n' = \frac{n}{m}$ völlig bestimmt.

Hieraus ergibt sich außerdem, daß m ein Teiler von n ist (vgl. die Bemerkung zu Beginn von Abschnitt III. 1).

Nach (3) ist auf diese Weise die Norm $[x]$ eindeutig als $[x] = N^{n'}(x)$ bestimmt.

Damit ist auch die *Realisierung* schon gegeben

b) M *sei nicht-kommutativ, d. h. eingebettet in eine Divisionsalgebra* $\mathfrak{D}/\mathsf{P}$ *mit dem Zentrum* $\mathfrak{K}$. $[\mathfrak{D}:\mathfrak{K}] = n_2^2$; $[\mathfrak{K}:\mathsf{P}] = n_1$; $n_1 \cdot n_2 = n$.

In diesem Fall beachte man die Tatsache, daß die Funktion $[x]$ als eine solche in den maximalen kommutativen Teilkörpern angesehen werden kann, denn jeder in $\mathfrak{D}$ enthaltene Körper ist in einem solchen enthalten (vgl. ALBERT [1], S. 57).

Für die maximalen kommutativen Teilkörper $\mathfrak{T}$ vom Grad m über P ist nach dem Obigen die Normfunktion $[x]$ eindeutig als $[x] = N^{n'}_{\mathfrak{T}/\mathsf{P}}(x)$ $(n = n'\,m)$ bestimmt. Es ist also $[x]$ in $\mathfrak{D}$ eindeutig als die n'-te Potenz der Hauptnorm $N^{n'}_{H}(x) = [x]$ bestimmt und damit auch realisiert.

Aus dem eben Gezeigten folgt, daß umgekehrt auch jede Ordnung in einem Zahlkörper vom Grad $m(m|n)$ bzw. in einer Divisionsalgebra mit den angegebenen Gradeigenschaften und separablem Zentrum $\mathfrak{K}$ ein Ring M ist, in dem die Norm die Axiome (A_1), (A_2) und (A_3) erfüllt. Andererseits war in den Abschnitten II und III abgeleitet worden, daß jeder Ring M mit diesen Eigenschaften isomorph zu einer Ordnung in einem Zahlkörper bzw. einer Divisionsalgebra ist. Deshalb sind als *Ringe* M *mit den bisher betrachteten Eigenschaften bis auf Isomorphie nur solche Ordnungen möglich.*

Es sei noch bemerkt, daß durch den Nachweis der Normenadditionsformel für die Körpernorm sofort die Hauptgleichung eines Elementes angegeben werden kann, wenn man die Normen der Elemente kennt. Es ist nämlich die Gleichung $X(\zeta) = 0$, wie sie in Abschnitt II hergeleitet ist. Die Koeffizienten der Gleichung sind dann Summen aus Normen, die hier ohne Benutzung der Interpolationsformeln gewonnen werden können.

Speziell sei die *Spur von* x durch eine solche Summe von Normen ausgedrückt. Es ist nämlich $|Spx| = n(x, 1, \ldots, 1)_n$.

Andererseits ist

$$n!(x, 1, \ldots, 1)_n = \sum_{\nu=1}^{n} (-1)^{n-\nu} \sum_{\varkappa \in \mathfrak{K}_\nu(n)} [x_{i_1} + \cdots + x_{i_\nu}].$$

Es gibt $\binom{n-1}{\nu-1}$ Kombinationen $\varkappa \in \mathfrak{K}_\nu(n)$, in denen x vorkommt, deren zugehöriges Glied $[x_{i_1} + \cdots + x_{i_\nu}]$ von der Form $[x + \nu - 1]$ ist. Außerdem gibt es $\binom{n}{\nu} - \binom{n-1}{\nu-1} = \binom{n-1}{\nu}$ Kombinationen aus $\mathfrak{K}_\nu(n)$, in denen x nicht auftritt, so daß das zugehörige Normenglied gleich $[\nu]$ ist.

Damit wird

$$\begin{aligned} &n!(x, 1, \ldots, 1)_n \\ &\quad = \sum_{\nu=1}^{n} (-1)^{n-\nu} \left\{ \binom{n-1}{\nu-1} [x + \nu - 1] + \binom{n-1}{\nu} [\nu] \right\} \\ &\quad = \sum_{\nu=1}^{n} (-1)^{n-\nu} \binom{n-1}{\nu-1} [x + \nu - 1] - \sum_{\nu=1}^{n-1} (-1)^{n-1-\nu} \binom{n-1}{\nu} [\nu], \end{aligned}$$

d. h. für Spx:

$$\begin{aligned} |Spx| &= \frac{n!}{(n-1)!}(x, 1, \ldots, 1)_n = \frac{1}{(n-1)!} \times \\ &\quad \times \left\{ \sum_{\nu=1}^{n} (-1)^{n-\nu} \binom{n-1}{\nu-1} [x + \nu - 1] - \sum_{\nu=1}^{n-1} (-1)^{n-1-\nu} \binom{n-1}{\nu} [\nu] \right\}. \end{aligned}$$

Bezeichnet man mit $\Delta^k f(x)$ die k-te Differenz der Funktion $f(x)$ an der Stelle x, wenn äquidistante Abstände 1 genommen werden, so kann man das auch in folgender Form schreiben:

$$Sp\, x = \frac{1}{(n-1)!}\{\Delta^{n-1}[x] - \Delta^{n-1}[0]\}.$$

V. Zusatzaxiome

Im Hinblick darauf, daß M als Multiplikatorenring eines algebraischen Funktionenkörpers vermutet wird, interessiert es noch, für M *zusätzliche Voraussetzungen* zu stellen, die für das Geschlecht 1 erfüllt sind (vgl. Deuring [3], 2. Teil).

1. (A_4) *Die Norm* $[x]$ *sei stets* $[x] \geqq 0$ *für alle* x *aus* M.

Dann ist sofort die Beziehung $[-x] = [x]$ abzuleiten.

Denn es ist $[-1] \geqq 0$; $[-1][-1] = [1] = 1$, also $[-1] = 1$.

Damit ist aber $[-x] = [x]$ nach (A_1).

Weiterhin folgt dann aus (R_8) in Verbindung mit (R_{10}) für ganzrationale a, b:

$$[ax + by] = (ax + by, \ldots, ax + by)_n = \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu} (\underbrace{x, \ldots, x}_{\nu}, \underbrace{y, \ldots, y}_{n-\nu}) \geqq 0.$$

Setzt man darin $a = -|a|$ und $y = 1$, so folgt, wenn außerdem durch $(-|a|)^n$ dividiert wird:

$$\sum_{\nu=0}^{n} (-1)^{n-\nu} \binom{n}{\nu} \left(\frac{b}{|a|}\right)^{n-\nu} (\underbrace{x, \ldots, x}_{\nu}, \underbrace{1, \ldots, 1}_{n-\nu}) \quad \begin{cases} \geqq 0 & \text{für } n \text{ gerade,} \\ \leqq 0 & \text{für } n \text{ ungerade.} \end{cases}$$

$\frac{b}{|a|} = \xi$ ist eine beliebige rationale Zahl. Es wird also für jede rationale Zahl ξ:

$$(U) \quad \sum_{\nu=0}^{n} (-1)^{n-\nu} \binom{n}{\nu} \xi^{n-\nu} (\underbrace{x, \ldots, x}_{\nu}, \underbrace{1, \ldots, 1}_{n-\nu}) \quad \begin{cases} \geqq 0 & \text{für } n \text{ gerade,} \\ \leqq 0 & \text{für } n \text{ ungerade.} \end{cases}$$

Auf der linken Seite steht aber das Polynom $X(\zeta)$ mit dem Argumentwert $\zeta = \xi \in \mathsf{P}$, wenn $X(\zeta) = 0$ die Gleichung für ein beliebiges Element $x \in \mathsf{M}$ ist, die in Abschnitt II abgeleitet wurde. Das Polynom hat reelle (sogar ganzrationale) Koeffizienten.

Für ungerades n kann diese Ungleichung nicht für alle rationalen ξ erfüllt sein, denn es muß ja mindestens ein Vorzeichenwechsel auftreten. Durch (A_4) scheiden also alle ungeraden n als mögliche Gradzahlen aus, und es muß $n = 2t$ sein.

Für $n = 2t$ bedeutet (U) aber, daß reelle Wurzeln der Gleichung $X(\zeta) = 0$ nur in geradzahliger Vielfachheit auftreten können. Dabei war $x \in \mathsf{M}$ beliebig.

Ist $n = 2$, so ist (U) die Ungleichung, aus der man die Schwarzsche Ungleichung für das innere Produkt von Vektoren ableitet. In diesem Falle folgt, daß das Polynom $X(\zeta)$ über P entweder ganz zerfällt (d. h. nur ganze rationale Nullstellen besitzt) oder ein Paar konjugiert-komplexer Nullstellen besitzt. Der Zahlkörper $\mathfrak{Z}$, in den M eingebettet werden kann, ist dann P oder ein ima-

ginär-quadratischer Zahlkörper. Das letztere ist dann auch für die maximalen kommutativen Unterkörper $\mathfrak{T}$ von $\mathfrak{D}$ (im nicht-kommutativen Fall) erfüllt. (Vgl. Deuring [3], 2. Teil; Behrbohm [2].)

Zieht man jetzt die Realisierung von $[x]$ durch $[x] = N^{n'}(x)$ aus dem Abschnitt IV heran, so kommt man nun zur *Beschreibung der möglichen Typen* von *Zahlkörpern* bzw. zu *Bedingungen* für die *Divisionsalgebren* $\mathfrak{D}$, in die M *eingebettet* werden kann, wenn für M neben den Axiomen (A_1), (A_2) und (A_3) noch (A_4) erfüllt ist.

Ist z. B. $m = n$ und $\mathfrak{Z} = \mathsf{P}(x)$ vom Grad n über P, so muß $\mathfrak{Z}$ ein total-imaginärer Zahlkörper[1]) sein. Ist M nicht-kommutativ, so muß jeder maximale kommutative Unterkörper von $\mathfrak{D}$ von diesem Typ sein.

Da die Norm eines Elementes y aus einem Körper $\mathfrak{K}/\mathsf{P}$ das Produkt seiner Konjugierten (mit der richtigen Vielfachheit genommen) ist, ist die Norm in total-imaginären Körpern immer positiv. Ist $\mathfrak{K}$ nicht total-imaginär, so kann man nicht ohne weitere Untersuchungen allgemeine Aussagen machen, außer folgender: Ist die Anzahl der zu z $(\mathfrak{K} = \mathsf{P}(z))$ reellen Konjugierten ungerade, so ist sicher $N(y) = -N(-y)$ und damit die Norm nicht immer positiv.

Mit den in den Abschnitten III und IV benutzten Bezeichnungen sei allgemein $[x] = N^{n'}(x)$; $n = m \cdot n'$. Dann ergibt sich folgende Einteilung:

1. M *kommutativ, eingebettet in* $\mathfrak{Z}/\mathsf{P}$; $[\mathfrak{Z}:\mathsf{P}] = m$.
   a) n' gerade.
      Hier ergibt sich keine Bedingung für $\mathfrak{Z}$.
      Es ist $N^{n'}_{\mathfrak{Z}/\mathsf{P}}(x) \geqq 0$, weil $N_{\mathfrak{Z}/\mathsf{P}}(x)$ aus P und n' gerade ist.
   b) n' ungerade.
      $\mathfrak{Z}$ muß total-imaginär sein.
      Denn hat die irreduzible Gleichung $g(\zeta) = 0$ für x $(\mathfrak{Z} = \mathsf{P}(x))$ reelle Wurzeln, so treten diese in $X(\zeta) = 0$, da n' ungerade ist, in ungerader Vielfachheit auf, entgegen der obigen Bedingung, die aus (U) folgt.
      Es ist ja $X(\zeta) = g^{n'}(\zeta)$, wie man aus den obigen Bemerkungen in Abschnitt IV. 1 über die Darstellung von $\mathfrak{Z}$ vom Grad n bzw. $[x] = N^{n'}_{\mathfrak{Z}/\mathsf{P}}(x)$ entnimmt.
2. M *nicht-kommutativ, eingebettet in* $\mathfrak{D}/\mathsf{P}$; $[\mathfrak{D}:\mathfrak{K}] = m_2^2$; $[\mathfrak{K}:\mathsf{P}] = m_1$; $m_1 \cdot m_2 = m$; $[x] = N^{n'}_{H}(x)$; $n = m \cdot n'$.
   a) n' gerade.
      Es tritt keine Bedingung weiter auf.
   b) n' ungerade.
      Alle maximalen kommutativen Unterkörper müssen total-imaginär sein.

Das folgt aus der schon öfter benutzten Tatsache, daß die Hauptnorm als Norm in jedem maximalen kommutativen Unterkörper betrachtet werden kann.

Diese eben bezeichneten Typen sind auch wirklich die einzigen, die möglich sind, weil die Norm $[x]$ eindeutig bestimmt ist.

2. (A_5) *Existenz eines involutorischen Antiautomorphismus.*

---

[1]) Das heißt, ist $\mathfrak{Z} = \mathsf{P}(x)$, so sind x und seine sämtlichen Konjugierten komplexe Zahlen.

Wie DEURING [3], 2. Teil, für $g = 1$ gezeigt hat, existiert in dem dort betrachteten Multiplikatorenring ein involutorischer Antiautomorphismus.

Es soll daher als zweite Zusatzforderung die Existenz eines solchen gestellt werden, um zu untersuchen, welche einschränkenden Bedingungen daraus für die Zahlkörper $\mathfrak{Z}$ bzw. die Divisionsalgebren $\mathfrak{D}$, in denen M Ordnung sein kann, folgen. Dabei denke man sich den involutorischen Antiautomorphismus in M auf $\mathfrak{Z}$ bzw. $\mathfrak{D}$ fortgesetzt, so daß man die Untersuchung gleich in $\mathfrak{Z}$ bzw. $\mathfrak{D}$ vornehmen kann.

Unter einem *involutorischen Antiautomorphismus* I von $\mathfrak{D}$ (der kommutative Fall ist darin enthalten) versteht man eine eineindeutige Abbildung von $\mathfrak{D}$ auf sich selbst mit den Eigenschaften $(a^I)^I = a$ und $(a \cdot b)^I = b^I \cdot a^I$ (vgl. ALBERT [1], Ch. X, auch für das Folgende).

Unter einem *symmetrischen* Element bei I ist ein Element mit der Eigenschaft $a^I = a$, unter einem *antisymmetrischen* ein solches mit $b^I = -b$ gemeint.

Sei nun $\mathfrak{A}$ eine Algebra mit einem solchen involutorischen Antiautomorphismus I, so ist I auch ein solcher des Zentrums $\mathfrak{K}$ von $\mathfrak{A}$. $\mathfrak{A}$ heißt *I-involutorisch von 1. Art*, wenn das Zentrum $\mathfrak{K}$ nur aus symmetrischen Elementen besteht und von *2. Art*, wenn $\mathfrak{K}$ auch nicht-symmetrische Elemente enthält.

In ALBERT [1], Ch. X, ist bewiesen, daß im Falle eines involutorischen Antiautomorphismus von 2. Art der Unterkörper $\mathfrak{S}$ der symmetrischen Elemente aus $\mathfrak{K}$ ein solcher Unterkörper ist, über dem $\mathfrak{K}$ separabel vom Grad 2 wird. Dabei ist für Charakteristik verschieden von zwei der Körper $\mathfrak{K}$ durch Adjunktion eines Elementes q mit den Eigenschaften $q^I = -q$; $q^2 = \alpha \in \mathfrak{S}$ zu erzeugen.

In dieser Arbeit liegt nun der Fall vor, daß die Divisionsalgebra $\mathfrak{D}$ normal einfach über einem endlichen algebraischen Zahlkörper ist. Daher ergeben sich nach ALBERT [1], Ch. X, S. 161ff., für die Körper $\mathfrak{Z}$ bzw. die Divisionsalgebren $\mathfrak{D}$, in denen M eine Ordnung sein kann, folgende notwendigen und hinreichenden *Bedingungen*, wenn neben den Axiomen (A_1), (A_2), (A_3) auch (A_5) (d. h. die *Existenz* eines *involutorischen Antiautomorphismus* I) erfüllt ist:

1. M *kommutativ, d. h. Ordnung in* $\mathfrak{Z}/\mathsf{P}$.
   a) Involutorischer Antiautomorphismus I von 1. Art (d. h. $\mathfrak{Z}$ besteht nur aus symmetrischen Elementen).
      Es besteht keine Einschränkung für $\mathfrak{Z}$.
   b) $\mathfrak{Z}$ sei I-involutorisch von 2. Art.
      $\mathfrak{Z}$ muß von der Form $\mathfrak{Z} = \mathfrak{S}(q)$ sein, d. h. $\mathfrak{Z}$ muß einen Unterkörper $\mathfrak{S}$ enthalten, über dem er quadratisch ist.
2. M *nicht-kommutativ, d. h. Ordnung in* $\mathfrak{D}/\mathsf{P}$.
   a) $\mathfrak{D}$ sei I-involutorisch von 1. Art.
      $\mathfrak{D}$ ist vom Grad 2 über seinem Zentrum $\mathfrak{K}$, d. h. eine Quaternionendivisionsalgebra.
   b) $\mathfrak{D}$ sei I involutorisch von 2. Art.
      $\mathfrak{D}$ muß eine zyklische Divisionsalgebra von folgendem Typ sein (Theorem 22, S. 162, bei ALBERT [1]):
      Ist $\mathfrak{D} = (\mathfrak{T}, S, \gamma)$ eine zyklische Algebra (daß $\mathfrak{D}$ von diesem Typ ist, ist schon aus Abschnitt III bekannt) d. h. $\mathfrak{D} = \mathfrak{T} + y\mathfrak{T} + \cdots$

$+ y^{m_2-1}\mathfrak{T}$; $y^{m_2} = \gamma \in \mathfrak{K}$; S erzeugendes Element der zyklischen Gruppe von $\mathfrak{T}/\mathfrak{K}$; $zy = yz^S$ für $z \in \mathfrak{T}$, so muß $\mathfrak{T} = \mathfrak{X} \times \mathfrak{K}$ sein und in $\mathfrak{X}$ muß ein Element x existieren, das die Normbedingung $N_{\mathfrak{K}/\mathfrak{S}}(\gamma) = N_{\mathfrak{X}/\mathfrak{S}}(x)$ erfüllt.

Aus der Einbettung von M in $\mathfrak{Z}$ bzw. $\mathfrak{D}$ kann man entnehmen, daß es vom involutorischen Antiautomorphismus in M abhängt, ob $\mathfrak{Z}$ bzw. $\mathfrak{D}$ I-involutorisch von 1. oder 2. Art sind. Enthält das Zentrum Z von M nur symmetrische Elemente, so liegt in $\mathfrak{Z}$ bzw. $\mathfrak{D}$ ein involutorischer Antiautomorphismus von 1. Art vor, sonst nicht.

Es ist nun zu untersuchen, ob die Forderung des involutorischen Antiautomorphismus nicht schon aus den gegebenen Axiomen (evtl. mit dem Zusatz (A_4) $[x] \geqq 0$) folgt.

Das ist nicht der Fall. Ist I von 1. Art, so kann man nämlich im nichtkommutativen Fall aus (A_1), (A_2), (A_3) und (A_4) nicht erschließen, daß $\mathfrak{D}$ vom Grad 2 über $\mathfrak{K}$ ist.

Für einen involutorischen Antiautomorphismus von 2. Art ist es durch folgendes Beispiel nachzuweisen:

Man wähle $\mathfrak{S} = \mathsf{P}$; $\mathfrak{K} = \mathsf{P}(i)$ d. h. $q = i$; $\mathfrak{X} = \mathsf{P}(i\sqrt{3})$ d. h. $\mathfrak{T} = \mathsf{P}(i, i\sqrt{3})$, außerdem $\gamma = 2 + i$. Betrachtet man dann die Algebra $\mathfrak{A} = (\mathfrak{T}, S, \gamma)$, so läßt sich zeigen, daß in $\mathfrak{X}$ kein Element x existiert, das der Normbedingung $N_{\mathfrak{K}/\mathfrak{S}}(\gamma) = N_{\mathfrak{X}/\mathfrak{S}}(x)$ genügt.

Da eben gezeigt wurde, daß (A_5) von (A_1), (A_2), (A_3) und (A_4) unabhängig ist, kann man die Unterabschnitte V. 1 und V. 2 zusammenfassen, und man erhält notwendige und hinreichende Bedingungen für $\mathfrak{Z}$ bzw. $\mathfrak{D}$, in denen M als Ordnung auftreten kann, wenn man nun für die Norm (A_1), (A_2), (A_3), (A_4) und (A_5) fordert.

A) *Der involutorische Antiautomorphismus I sei von 1. Art.*

1. M *kommutativ, d. h. Ordnung in* $\mathfrak{Z}/\mathsf{P}$:
   a) n' gerade: Keine Bedingung für $\mathfrak{Z}$,
   b) n' ungerade: $\mathfrak{Z}$ total-imaginär.
2. M *nicht-kommutativ, d. h. Ordnung in* $\mathfrak{D}/\mathsf{P}$:
   a) n' gerade: $\mathfrak{D}$ Quaternionendivisionsalgebra über $\mathfrak{K}$; $\mathfrak{K}$ beliebig,
   b) n' ungerade: $\mathfrak{D}$ Quaternionendivisionsalgebra über $\mathfrak{K}$; alle maximalen kommutativen Unterkörper total-imaginär.

B) *I sei von 2. Art.*

1. M *kommutativ*:
   a) n' gerade: $\mathfrak{Z} = \mathfrak{S}(q)$; $q^2 \in \mathfrak{S}$; $\mathfrak{S}$ beliebig,
   b) n' ungerade: $\mathfrak{Z} = \mathfrak{S}(q)$; $q^2 \in \mathfrak{S}$; $\mathfrak{S}$ total-imaginär.
2. M *nicht-kommutativ*:
   a) n' gerade: $\mathfrak{D}$ zyklisch $\mathfrak{D} = (\mathfrak{T}, S, \gamma)$ über $\mathfrak{K}$; $\mathfrak{T} = \mathfrak{K} \times \mathfrak{X}$ und Normbedingung $N_{\mathfrak{K}/\mathfrak{S}}(\gamma) = N_{\mathfrak{X}/\mathfrak{S}}(x)$,
   b) n' ungerade: $\mathfrak{D}$ zyklisch wie in a) und dazu: alle maximalen kommutativen Unterkörper total-imaginär.

Schlußbemerkung

Vergleich mit dem Vorgehen von Deuring in [3] *für* $g = 1$.

Ist $g = 1$, $2g = n = 2$, so hat DEURING [3] den Multiplikatorenring M, der den Axiomen $(A_1), \ldots, (A_5)$ genügt, behandelt, indem er *von der Existenz des Antiautomorphismus ausgeht.* In diesem Falle liegt aber das Produkt $x \cdot x^I$ immer im Grundkörper P, so daß man mit den symmetrischen Bildungen $x \cdot x^I$ und $x + x^I$ sofort die Gleichung 2. Grades für $x \in \mathsf{M}$ erhält. Durch den involutorischen Antiautomorphismus ist man dort außerdem in der Lage, die Norm als $[x] = x \cdot x^I$ zu erklären. Wie aus Abschnitt V zu ersehen ist, kann man im allgemeinen Fall $n > 2$ nicht so einfach vorgehen, denn das Produkt $x \cdot x^I$ genügt dann einer Gleichung vom Grad $k \geqq 1$ über P. Will man auch hier von der Existenz des involutorischen Antiautomorphismus ausgehen, so müßte man fordern, daß $x \cdot x^I$ immer einer Gleichung höchstens vom Grad k über P genügt. Dann wäre es möglich, M in eine Divisionsalgebra einzubetten. Die Norm $[x]$ könnte dann als Hauptnorm von $x \cdot x^I$ bzw. als Potenz dieser erklärt und die Normenadditionsformel als richtig nachgewiesen werden.

Erhält man also bei dem in dieser Arbeit eingeschlagenen Weg der Forderung der Norm mit ihren Eigenschaften (A_1), (A_2), (A_3) die Existenz der Gleichungen über P für jedes Element $x \in \mathsf{M}$, so muß man die Existenz der Gleichungen fordern (oder durch andere Forderungen nachweisen), wenn man die Normeneigenschaften ableiten will. Nur weil für $g = 1$ $x x^I$ einer Gleichung 1. Grades über P genügt, sind die Verhältnisse dort besonders einfach.

Literatur

[1] A. A. ALBERT, Structure of Algebras. New York 1939.

[2] H. BEHRBOHM, Über die Algebraizität der Meromorphismen eines elliptischen Funktionenkörpers. Nachr. Ges. Wiss. Göttingen, II. Ser., **1**, 131—134 (1935).

[3] M. DEURING, Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper I. J. reine angew. Math. **177**, 161—191 (1937). Teil II. J. reine angew. Math. **183**, 25—36 (1941).

[4] ———, Algebren. Ergebnisse der Math. **4**, Nr. 1 (1935), 143 S.

[5] H. HASSE, Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III. J. reine angew. Math. **175**, 55—62, 69—88, 193—208 (1936).

[6] P. ROQUETTE, Arithmetische Untersuchung des Abelschen Funktionenkörpers, der einem algebraischen Funktionenkörper höheren Geschlechts zugeordnet ist. Abh. math. Sem. Univ. Hamburg **18**, 144—178 (1952).

[7] H. L. SCHMID, Zur Meromorphismentheorie der elliptischen Funktionenkörper. Math. Z. **47**, 399—421 (1941).

[8] B. L. v. d. WAERDEN, Moderne Algebra I. 2. Aufl. Berlin 1937.

[9] A. WEIL, Sur les courbes algebriques et les variétés s'en deduisent. Actual. sci. industr. 1041. Paris 1948.

[10] E. WITT, Besprechung der Arbeit [2] von H. Behrbohm. Zentralblatt für Math. u. ihre Grenzgebiete **13**, S. 198 (1936).